PENGEMBANGAN KERANGKA KERJA MANAJEMEN KEAMANAN INFORMASI (STUDI EMPIRIK : UNIVERSITAS MUHAMMADIYAH SEMARANG)

Bambang Supradono*

** Teknik Elektro Fakultas Teknik Universitas Muhammadiyah Semarang*
E-mail: bsupradono@gmail.com

ABSTRAK

Penelitian ini bertujuan untuk membuat panduan kerangka kerja manajemen keamanan informasi sebagai solusi manajemen risiko keamanan informasi yang sistematik dan holistik. Kerangka kerja ini memiliki alur tahapan proses yang diawali dari membuat tahapan persiapan . Kemudian dilanjutkan dengan mengidentifikasi aset, kebijakkan dan dokumen pengelolaan keamanan informasi , operasional Teknologi Informasi (TI), jaringan komunikasi, pengamanan informasi serta Business Continuty Planning.

Langkah selanjutnya melakukan audit kelemahan infrastruktur baik hardware maupun software. Dari dua tahapan tersebut ditemukan kelemahan yang menjadi acuan solusi mitigasi/pengurangan risiko dengan ditindaklajuti pada tahapan rencana mitigasi risiko. Akhirnya solusi ancaman dan kelemahan dipetakan pada rencana-rencana taktis jangka pendek dan strategi proteksi manajemen keamanan jangka panjang dan akan terus dievaluasi secara berkesinambungan. Sehingga dari tahapan ini kan menjaga keberlanjutan proses bisnis.

Penelitian ini mengambil studi kasus pada proses bisnis Universitas Muhammadiyah Semarang yang berbasis teknologi informasi.

Dari hasil penelitian menunjukkan bahwa kerangka kerja mampu mendeskripsikan secara komprehensif karena melibatkan partisipasi seluruh penggung jawab TI dalam mengevaluasi kelemahan baik dari sisi teknologi dan kebijakkan. Serta mampu memberikan panduan operasional secara holistik dari level taktis hingga strategis. Mampu memberikan dukungan keberlanjutan proses bisnis dalam rangka mengantisipasi ancaman dan kelemahan yang terus berkembang.

Kata kunci: *Mitigasi risiko, Business Continuty Planning*

PENDAHULUAN

Untuk mencapai tujuan bisnisnya, seringkali perusahaan atau organisasi menggunakan Teknologi Informasi (TI) dalam mengelola informasi sebagai basis dalam penciptaan layanan yang berkualitas ataupun dalam optimalisasi proses bisnisnya. Meningkatnya tingkat ketergantungan organisasi pada sistem informasi sejalan dengan resiko yang mungkin timbul (Harris, et. all, 2008).

Salah satu risiko yang timbul adalah risiko keamanan informasi, dimana informasi menjadi suatu yang penting yang harus tetap tersedia dan dapat digunakan, serta terjaga keberadaannya dari pihak yang tidak berwenang yang akan menggunakannya untuk kepentingan tertentu atau akan merusak informasi tersebut. Informasi merupakan sebuah aset penting bagi organisasi (Nosworthy, 2000) yang perlu dilindungi dan diamankan.

Keamanan informasi tidak bisa hanya disandarkan pada tools atau teknologi keamanan informasi, melainkan perlu adanya pemahaman dari organisasi tentang apa yang harus dilindungi dan menentukan secara tepat solusi yang dapat menangani permasalahan kebutuhan keamanan informasi (Willett, 2008). Untuk itu butuh pengelolaan keamanan informasi yang sistemik dan komprehensif.

Institusi Perguruan Tinggi yang merupakan suatu enterprise yang bergerak di bidang industri pendidikan dimana proses bisnisnya perlu dukungan teknologi informasi untuk meningkatkan akses, kualitas serta menurunkan biaya layanan (Daniel, et. all, 2002). Disamping itu tuntutan perkembangan penyelenggaraan pendidikan yang berkualitas menuntut perguruan tinggi yang menggunakan teknologi informasi sebagai ciri pendidikan modern dewasa ini (Indrajit, 2006).

Terkait hal tersebut banyak proses bisnis pada institusi perguruan tinggi yang sarat dengan penerapan TI dimana salah satunya yang menjadi objek penelitian adalah sistem informasi di Universitas Muhammadiyah Semarang.

Sekarang ini sudah menjadi kecenderungan dan tuntutan bagi institusi perguruan tinggi menerapkan manajemen keamanan informasi terkait dengan informasi yang dipublikasi secara umum lewat internet. Dimana aset-aset informasi yang ada dalam sistem informasi (informasi, sistem, piranti lunak , piranti keras dan sumber daya manusia) perlu dilindungi risiko keamanannya dari ancaman dan kerentanan baik dari dalam *(inbound)* dan luar *(outbound)*, (Maria et.al, 2007) agar terjamin keberlanjutan proses bisnisnya.

METODE PENELITIAN

1. Bahan Penelitian

Adapun bahan penelitian berupa informasi yang diperoleh melalui dari berbagai sumber dengan cara melakukan :

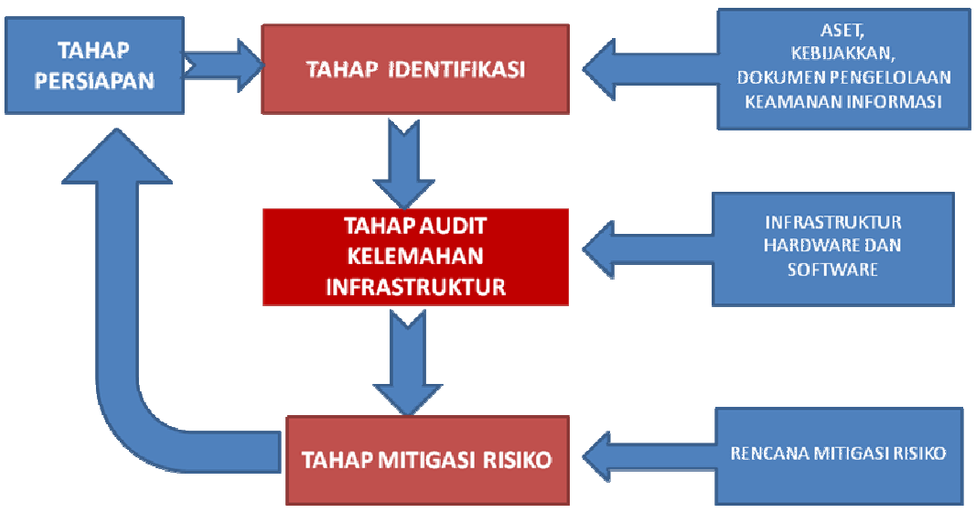
1. ***Membuat daftar kuesinoner***. Daftar kuesioner ini di susun untuk semua level manajemen yang terlibat dalam sistem dengan tujuan mengumpulkan informasi seputar praktek-praktek

2. keamanan informasi dengan tujuan untuk memperoleh pemahaman organisasi tentang keamanan informasi
3. ***Interview*****.** Bentuk lain dari pengumpulan data dengan cara interview terhadap pimpinan dan staf TI yang terlibat dalam sistem informasi untuk memperoleh pemahaman organisasi tentang kebutuhan keamanan informasi.
4. ***Pengamatan lapangan :*** Pengumpulan data mengamati secara langsung dengan cara mengujicoba dan mengevaluasi kelemahan infrastruktur jaringan komunikasi.
5. ***Review atas dokumen*****.** Review atas dokumen pengembangan sistem, Dokumen kebijakan, atau dokumen keamanan informasi dapat memberikan gambaran yang bermanfaat tentang bentuk dari kontrol yang saat ini diterapkan oleh SI maupun rencana pengembangan dari pengawasan di masa depan.

2. **Alat Penelitian**

1. ***Penerapan Tool/Utilitas*** **.** Menggunakan suatu tool/utilitas aplikasi yang memiliki tujuan untuk mengumpulkan informasi tentang audit sistem informasi yang digunakan merupakan salah satu cara untuk dapat memetakan sistem secara keseluruhan, dan menguji kelemahan teknologi yang digunakan seperti penggunakan network monitoring sistem, port scanner (Netmap. wireshark dll), drawing tools (MS Visio) maupun tools lain.
2. ***Instrumen Penelitian :*** Dokumen isian tentang aset, praktek-praktek keamanan dan kebijakkan organisasi. Dokumen ini mengadopsi dari pedoman Bank Indonesia dalam mengevaluasi kinerja manajemen risiko keamanan bank umum dan swasta.

3. Jalan Penelitian



Gambar 1. Diagram Alur Penelitian

Proses alur penelitian terdiri dari 4 tahapan meliputi :

1. **Tahap Persiapan** : Aktifitas di tahap ini meliputi penyusunan jadwal penelitian, menyiapkan tim audit, menyiapkan logistik penunjang penelitian (utilitas, instrumen penelitian dan administrasi), serta menetapkan sasaran responden penelitian.
2. **Tahap Identifikasi Aset, Kebijakkan, Dokumen Pengelolaan Keamanan Informasi** : Pada tahap ini aktifitas yang dilakukan adalah mengidentifikasi aset-aset informasi, mengaudit kebijakkan dan dokumen pengelolaan keamanan informasi dengan alat bantu instrumen penelitian.
3. **Tahap Audit Kelemahan infrastruktur** : pada tahap ini melakukan pengamatan langsung keberadaan infrastruktur sistem informasi baik perangkat keras (Router, Antena radio, Server, Wireless dan lain-lain) serta perangkat lunak (seperti firewall, network monitoring, enkripsi dan konten web).
4. **Tahap Mitigasi Risiko** : tahap ini adalah upaya rekomendasi mitigasi risiko dari kelemahan-kelemahan yang ditemukan pada tahap sebelumnya (tahap identifikasi dan tahap audit kelemahan infrastruktur). Output tahap ini merupakan rencana strategi mitigasi risiko yang menjadi pedoman perbaikan risiko ke depan dan tahap ini merupakan tahapan yang berkelanjutan dan upaya peningkatan mitigasi risiko secara terus menerus.

HASIL PENELITIAN DAN PEMBAHASAN

Pada hasil dan pembahasan menitik beratkan pada aspek tahap migrasi risiko dengan fokus pada kekurangan/kelemahan yang ditemukan pada tahap sebelumnya yakni tahap identifikasi dan tahap identifikasi kelemahan infrastruktur. Dari kelemahan ini kemudian memunculkan saran-saran perbaikan, sehingga memudahkan untuk mengevaluasi perbaikan secara berkelanjutan.

1. Rencana Mitigasi Risiko Terhadap Kebijakkan dan Dokumen Pengelolaan Keamanan

a. Mitigasi Risiko Kebijakkan Keamanan Informasi

Dari hasil survei kuesioner Dep. TIK dan PDPT UNIMUS diperoleh nampak pada tabel 1 perlu ada upaya perbaikan dengan melakukan mitigasi risiko pada tabel 1 di bawah ini :

Tabel 1. Hasil survei mitigasi kebijakkan manajemen keamanan informasi

Kebijakkan Keamanan Informasi	Catatan kelemahan	Mitigasi Risiko
Renjana jangka panjang TI	Belum memiliki dan Tidak Terlampir	Diupayakan membuat cetak biru rencana jangka panjang dan roadmap keamanan informasi
Job description TI	Ada Belum Terdokumentasi dan belum konsisten	Diupayakan untuk membuat SOP dan Instruksi kerja agar pekerjaan bisa konsisten, bisa dievaluasi aktifitas staf dan memudahkan konsolidasi bila ada rotasi staf
Pelatihan di bidang	Ada	Terus ditingkatkan kemampuan staf TI baik

keamanan yang penah diikuti personil TI	-Pelatihan Keamanan dan Pengelolaan Jaringan	secara kualitas dan kuantitas, lebaih baik lagi diupayakan magang pada institusi yang cakupan pekerjaannya lebih komplek.
Risk Management (Manajemen Risiko) a. Terdapat petugas untuk memonitor resiko terkait TI	Ada, tetapi tidak terlalu fokus karena banyak dibebani pekerjaan tambahan, sistem kerja tidak tersistematis, masih reaktif bila ada kejadian tidak prefentif	Petugas administrator seharusnya fokus pada monitoring ketersediaan dan kerahasiaan data dari ancaman manusia baik dari dalam/luar, mallicious code (virus, spam dll) yang dapat menganggu ketersediaan, kerahasiaan dan integritas sistem informasi.
b. Terdapat utilitas, sistem dan prosedur untuk memonitor resiko terkait TI di satuan kerja TI	Ada, tetapi *belum terdokumentasi* secara benar dan tidak dilakukan secara sistematis dan konsisten.	Perlu adanya upaya dokumentasi dalam merekam jejak aktifitas-aktifitas pengamanan untuk bisa dievaluasi dan ditingkatkan secara berkelanjutan, Memudahkan pengelolaan pengetahuan staf TI dalam medokuementasi aktifitas-aktifitasnya.
c. Terdapat analisis terkini dari identifikasi risiko, monitoring dan mitigasi risiko.	Belum dilakukan karena masih menganggap risiko dapat ditangani secara temporer	Perlu ada mekanisme kerja yang bersifat prefentif bagi staf TI tidak selalu bertindak reaktif

b. Mitigasi Risiko Operasional TI

Dari hasil instrumen penelitian identifikasi operasional TI nampak pada tabel 2. di bawah ini :

Tabel 2. Mitigasi Operasional TI

Operasional TI	Catatan Kelemahan	Mitigasi Risiko
Informasi Mengenai pusat data - Kelengkapan pengamanan fisik pusat data	Ada tetapi beberapa tidak difungsikan secara normal seperti genset, UPS, lantai belum raised floor, tata letak kabel masih acak, secara lokasi belum layak dipakai sebagai pusat data.	Perlu adanya standar ruang server/data center guna menjaga ketersediaan yang dapat dihandalkan karena server tulangpunggung aplikasi yang menunjang proses bisnis
Aplikasi khusus pengamanan informasi	Tidak Ada	Perlu direncanakan ruang server/data center diproteksi aturan yang boleh memasuki ruang server hanya staf TI yang berkepentingan, selain itu dilarang . Ada baiknya dilengkapi fasilitas kunci biometrik, seperti finger print
Prosedur penanganan masalah (Problem Handling)	Tidak Ada	Perlu ada upaya semacam fasilitas layanan bantu (helpdesk) staf TI dalam

		membantu gangguan dari layanan TI bagi pemakai.
Kebijakkan, sistem dan prosedur manajemen perubahan	Tidak Ada	Perlu dikembangkan manajemen perubahan terkait proses budaya penggunaan TI baik, sehat dan aman
Kebijakkan sistem dan prosedur pengelolaan hak akses pengguna sistem dan aplikasi	Tidak Ada	Perlu dikembangakan SOP pengelolaan hak akses pengguna
Kebijakkan, sistem dan prosedur back –up data	Ada, sifatnya manual	Diupayakan proses back up dilakukan secara berkala dan otomatis.

c. Mitigasi Risiko Jaringan Komunikasi

Dari hasil instrumen penelitian identifikasi jaringan komunikasi nampak pada tabel 3 di bawah ini :

Tabel 3. Mitigasi Risiko Jaringan Komunikasi

Jaringan Komunikasi	Catatan Kelemahan	Mitigasi risiko
Kebijakkan, sistem dan prosedur pengamanan jaringan	Tidak Ada	Perlu dibuat SOP pengamanan jaringan
Daftar perangkat keras dan lunak yang digunakan untuk jaringan	Ada dan Terlampir	Harus selalu mengupdate dan mendokemtasikan dalam katalog-katalog perangkat keras dan lunak.
Network Monitoring System	Ada, menggunakan DUDE Mikrotik, terlampir	Diupayakan admin selalu memonitoring kinerja jaringan pada awal atifitasnya.
Kebijakan untuk konfigurasi pengamanan komunikasi data (firewall)	Ada,	Perlu selalu update dan mendokumentasi bila ada aktifitas yang tidak normal, sehingga memudahkan dalam memproteksi keamanan.

d. Mitigasi Risiko Aplikasi dan Pengembangan.

Dari hasil instrumen penelitian identifikasi operasional TI dengan responden PDPT nampak pada tabel 4 di bawah ini :

Tabel 4. Mitigasi Risiko Aplikasi dan Pengembangan

Aplikasi dan Pengembangan	Catatan kelemahan	Mitigasi Risiko
Kebijakkan dan prosedur pengembangan aplikasi dilakukan dengan universitas.	Tidak Ada	Perlu ada upaya dokumentasi setiap pengembangan aplikasi meliputi, kamus data, ER diagram, database management system, source code dan algoritma.
Apakah universitas memiliki fungsi	Belum ada	Perlu direncanakan kedepan bahwa

project management untuk aplikasi yang sedang dikembangkan		proyek software juga perlu dikelola secara proyek sehingga proyek dapat berjalan *on-schedule* dan terkontrol.

e. Mitigasi Risiko Pengamanan Informasi.

Dari hasil instrumen penelitian identifikasi pengamanan informasi dengan responden Dep. TIK nampak pada tabel 5 di bawah ini :

Tahap 5. Identifikasi Pengamanan informasi

Pengamanan informasi	Catatan Kelemahan	Mitigasi Risiko
Kebijakkan dan prosedur pengamanan informasi mencakup :		
- Security Awareness Program	Belum Ada	Perlu upaya menbangun budaya bagi staf TI untuk menjaga keamanan. Juga perlu ada upaya kampanye penggunaan internet yang aman bagi user. Perlu upaya mekanisme pengananan kejadian yang tidak diinginkan yang dapat menggangu aspek keamanan
- Incident handling	Belum Ada	Perlu direncanakan untuk menjaga jaga admin lupa login yang biasa digunakan , emergency semacam login duplikat buat admin
- Penggunaan software legal - Pencegahan penggunaan software ilegal	Belum Ada	Perlu ada kebijakkan penggunaan software legal, perlu dukungan seluruh sivitas akademika dari rektor hingga pimpinan program studi. Selain itu solusi software legal murah dengan membuat *campus agrement* dengan vendor software.
Pengelolaan asset - Pengamanan fisik termasuk penggunaan alat pengamanan	Tidak Ada	Perlu diupayakan ruang server/data center menggunakan alat pengaman seperti finger print, CCTV dll
Pengamanan Akses - Penerapan pengamanan password pada aplikasi misal aplikasi telah memaksa user untuk mengubah password secara berkala.	Belum Ada	Perlu ada upaya manajemen password yang baik (Perubahan setiap 30/60/90 hari, dibuat standar minimal 8 karakter dan unik untuk password, admin menggunakan password generator, melarang penggunaan login admin sebagai demo login dll).
- Terdapat fungsi audit log untuk setiap aktifitas yang	Belum Ada	Perlu ada mekanisme rekam jejak aktifitas konfigurasi yang dilakukan admin/user untuk memonitor aktifitas-aktifitas yang tidak diinginkan.

- dilakukan user dan dilakukan analisa terhadap audit log. - Review secara periodik terhadap kesesuaian user	Ada, sudah dilakukan tiap 2 bulan	
Sumber daya manusia - Ketentuan mengenai pengamanan informasi dengan staf, pegawai magang, dan pihak ketiga - Adanya ketentuan mengenai sanksi atas pelanggaran terhadap kebijakkan pengamanan informasi - Prosedur pengembalian atau perubahan hak akses terhadap aset terkait informasi saat terjadi perubahan perjanjian	Belum Ada, padahal terkadang ada pelajar SMK yang magang Belum ada, Belum Ada	Membuat prosedur kolaburasi pengaturan keamanan dengan pihak ketiga dan membatasi akses ke sistem bagi siswa magang Perlu sosialisasi payung hukum UU ITE no 11 th 2008. Tentang aspek jaminan kepastian hukum bagi staf yang mencoba mengganggu sistem informasi.
Pengamanan fisik termasuk penggunaan alat pengaman (PIN dll) terhadap pemrosesan informasi	Belum Ada	Perlu diupayakan penambahan pengamana fisik untuk mencegah gangguan secara phisik bagi server.
Operasional aplikasi : Ketentuan mengenai pengamanan dalam identifikasi dan otentifikasi akses misal : Password, token, biometric dll.	Belum Ada	Perlu ada penambahan peralatan akses elektronik seperti token , biometrik dll pada akses ruangan server
Prosedur pelaporan inseden pengamanan informasi dan tindak lanjutnya.	Belum Ada	Perlu ada sistem pelaporan dan dokumentasi terhadap insiden ancaman keamanan sehingga dapat dimonitoring dan evaluasi

f. Mitigasi Risiko BCP (*Bussines Continuity Planning)*

Dari hasil instrumen penelitian identifikasi pengamanan informasi dengan responden Dep. TIK nampak pada tabel 6 di bawah ini :

Tabel 6. Identifikasi BCP (*Bussines Continuity Planning)*

Bussines Continuity Planning	**Catatan Kelemahan**	**Mitigasi Risiko**
Kebijakkan, sistem dan prosedur *bussiness continuty plan* termasuk *disaster recovery plan* di dalamnya Apakah universitas memiliki	Belum Ada	Perlu dibuat rencana DCP untuk menjaga

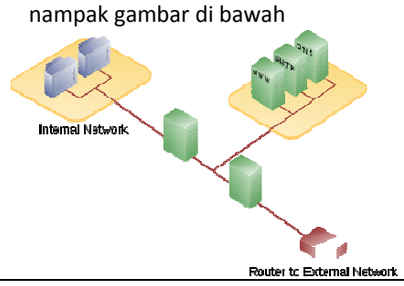
disaster recovery plan (DCP):		ketersedian layanan yang berkesinambungan, bila suatu saat terjadi kejadian force major/bencana alam
Struktur organisasi dan kewenangan Bussiness continuty plan	Belum Ada	Mengingat keterbatas anggaran TI sehingga belum bisa mengganggarkan infrastruktur penujang BCP Perlu upaya kebijakkan untuk menjaga keberlanjutan proses
Testing BCP dan DRP Kebijakkan, sistem dan prosedur testing	Tidak Ada	Perluada upaya mekanisme BCP dan DRP untuk menjaga keberlanjutan proses bisnis salah satu solusinya adalah membuar server miror tidak pada satu lokasi yang sama dengan server inti.

g. Mitigasi Resiko Kelemahan Infrastruktur

Dari hasil analisis audit kelemahan infrastruktur maka disusun rencana strategi mitigasi risiko pada kelemahan infrastruktur, nampak pada tabel 7 di bawah ini :

Tabel 7. Mitigasi Risiko Kelemahan Infrastrukur

Infrastruktur	**Catatan Kelemahan**	**Mitigasi Risiko**
Antena Radio Komunikasi data Wide Area Network	Posisi ketinggian antena < 40 m	Perlu ada solusi penguatan penangkal petir, karena peralatan penangkal petir saat ini belum optimal melindungi dari serangan pettir, jika koneksi lebih stabil solusinya adalah menyewa layanan komunikasi data pihak Telkom dengan Fiber Optik
Server	Ruang server tidak standar dan utilitas pendukung server belum optimal seperti genset, penataan kabel, redundansi daya listrik.	- Ruang server perlu di bangun *lay out* tempat model raised floor. - Konfigurasi kabel harus ditata rapi supya mudah melakukan problem handling - Ruang kantor hendaknya terpisah dari ruang server, supya aktyifitas kantor tidak mengganggu keberadaan server. - Perlu genset sebagai pendukung ketika listrik PLN Off. - Server perlu dukungan redundancy catu daya. - Server ditempatkan dengan sistem DMZ (De-Militarized Zone) itu semacam zona di network topology yang fungsinya untuk mengamankan jaringan. Zona tersebut biasanya berisi server farm (kumpulan server2 kayak web server, mail server, proxy server, dll) dan memiliki koneksi ke dalam LAN maupun Internet. jadi paket2

		- yang ingin melalui LAN harus melalui DMZ dulu. kira2 begitu. DMZ bisa di setting melalui firewall atau network device yang capable.
Konten dan Aplikasi Sistem Informasi	Tidak ada,	- Perlu direncanakan teknik enkripsi melibatkan pihak ketiga sebagai pihak penjamin kerahasiaan data dengan teknik enkripsi yang bisa dihandalkan seperti verisgn dll. - File-flie yang dipublikasi status properti filenya hanya bisa baca sehingga terlindungi dari modifikasi pihak-pihak yang tidak berkepentingan
Jaringan Hotspot	Tidak Ada	- Sudah memiliki server radius AAA server untuk melayani authentikasi, authorisasi dan akunting user login, sehingga jaringan hotspot keamanaannya bisa dihandalkan.
Firewall	Sudah memiliki namun monitoringnya tidak terjadwal dan respon penanganan masalahnya tidak cepat	- Perlu upaya penjadwalan monitoring firewall yang sistematis dan terjadwal - Perlu mekanisme *problem handling* yang cepat,tanggap dan tepat. - Perlu dokuemtasi insiden-insiden yang menimbulkan gangguan keamanan sehingga mudah untuk evaluasi dan monitoring. - Perlu ada konfigurasi jaringan dengan pertahanan berlapis dalam memasang firewall dengan model firewall ganda nampak gambar di bawah 

SIMPULAN

Hasil isolasi dan identifikasi bakteri pada kultur darah Widal positif asal Kota Semarang berdasarkan karakter fenotipik menggunakan media API 20E, API 50 CHB/E dapat diketemukan bakteri batang gram negatif anggota familia *Enterobacteriaceae* yaitu: *Enterobacter cloacae, S. typhi, Serratia marcescens, Escherichia coli, Salmonella* ssp., *Klebsiella pneumoniae* ssp. Ozanae. Hasil identifikasi bakteri menggunakan API Stap adalah: *S. aureus, S. saprophyticus, S. xylosus, S. warnei*, *S. hominis, S. cohnii.*

Berdasarkan karakter fenotipik bakteri batang gram negatif dapat dikelompokkan menjadi 4 kluster, kluster pertama beranggotakan *S. typhi* , kluster kedua beranggotakan *E. coli* dan *Salmonella* ssp., kluster ketiga beranggotakan *Ser. marcescens* dan kluster keempat beranggotakan *Enterobacter cloacae* dan *Kleb. pneumoniae* ssp. Ozaenae. Bakteri kokus gram positif berdasarkan karakter fenotipiknya dapat dikelompokkan menjadi 6 kluster yang tampak sangat bervariasi.

UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih kepada Lembaga Penelitian yang telah memberikan dana untuk penelitian Internal tahun anggaran 2011.

DAFTAR PUSTAKA

Christhoper J Alberts, A. J. D. (2001) Managing Information Security Risk, The OCTAVESM Approach Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

Herbert J. Mattord, M. W. (2004). Principles of Information Security, Course Technology Ptr.

Indrajit, R. (2006). Manajemen Perguruan Tinggi Modern, Andi Offset.

Maria Nickolova, E. N. (2007). "Threat Model for User Security in E-Learning Systems." Information Technologies and Knowledge **1**.

Michael D. Harris, D. E. H., Stasia Iwanicki (2008). The Businness Value of IT, Auerbach Publications Taylor and Francis Group.

Nosworthy, J. D. (2000). "Implementing Information Secutiry in the 21st Century - Do you have the balancing actors?" Computer dan Security **19**: 337-347.

Willet, K. D. (2008). Information Assurance Architecture, Auerbach Publications Taylor and Francis Group.